

JASON R. HULL [11202]
JHULL@MOHTRIAL.COM
MARSHALL OLSON & HULL, PC
TEN EXCHANGE PLACE, SUITE 350
SALT LAKE CITY, UTAH 84111
TELEPHONE: 801.456.7655

MASON A. BARNEY*
MBARNEY@SIRILLP.COM
TYLER J. BEAN*
TBEAN@SIRILLP.COM
SIRI & GLIMSTAD LLP
745 FIFTH AVENUE, SUITE 500
NEW YORK, NEW YORK 10151
TELEPHONE: 212.532.1091

ATTORNEYS FOR PLAINTIFFS AND
PROPOSED CLASS COUNSEL

*PRO HAC VICE FORTHCOMING

**IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, CENTRAL DIVISION**

<p>MANDY KEASLER, on behalf of herself, her minor son, A.K., and all others similarly situated,</p> <p>Plaintiffs,</p> <p>v.</p> <p>UINTAH BASIN HEALTHCARE d/b/a UINTAH BASIN MEDICAL CENTER</p> <p>Defendant.</p>	<p>COMPLAINT</p> <p>[PROPOSED CLASS ACTION]</p> <p>JURY TRIAL DEMANDED</p> <p>Case No.: 2:23-cv-00323</p>
---	--

CLASS ACTION COMPLAINT

Plaintiffs Mandy Keasler, on behalf of herself and her minor son, whose initials are A.K., individually and on behalf of all similarly situated persons, allege the following against Uintah Basin Healthcare d/b/a Uintah Basin Medical Center (“Uintah” or “Defendant”) based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

INTRODUCTION

1. Plaintiffs bring this class action against Uintah for its failure to properly secure and safeguard Plaintiffs' and other similarly situated current and former Uintah patients' personally identifiable information ("PII") and protected health information ("PHI"), including names, dates of birth, addresses, Social Security numbers, health insurance information, and certain clinical details including diagnosis/conditions, medications, test results, and procedure information (the "Private Information"), from criminal threat actors.

2. Uintah Basin Healthcare, based in Roosevelt, Utah, is a hospital that serves tens of thousands of patients annually.

3. On or about May 10, 2023, Uintah also sent out data breach letters to individuals whose information was compromised as a result of the hacking incident.

4. Based on the Notice sent to victims, including Plaintiffs, unusual activity was detected on its network on or around November 7, 2022 (the "Data Breach"). Uintah's investigation revealed that an unauthorized party may have accessed and acquired Plaintiff's and "Class Members'" (defined below) Private Information as a result, yet Uintah waited roughly *six months* to notify them that they were at risk.

5. As a result of this delayed response, Plaintiffs and Class Members had no idea for months that their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

6. The Private Information compromised in the Data Breach contained highly sensitive patient data, representing a gold mine for data thieves. The data included, but is not limited to, names, Social Security numbers, dates of birth, medical treatment information, and

health insurance information that Uintah collected and maintained from patients who, according to the Notice letter, “received care with [Uintah] between March 2012 and November 2022.”

7. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members’ names, taking out loans in Class Members’ names, using Class Members’ names to obtain medical services, using Class Members’ information to obtain government benefits, filing fraudulent tax returns using Class Members’ information, obtaining driver’s licenses in Class Members’ names but with another person’s photograph, and giving false information to police during an arrest.

8. There has been no assurance offered by Uintah that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future. Nor did Uintah offer any remedial assistance to the victims of the Data Breach (some of whom are very young children) other than a woefully inadequate twelve (12) months of free credit monitoring.

9. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

10. Plaintiffs bring this class action lawsuit to address Uintah’s inadequate safeguarding of Class Members’ Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiffs and Class Members of the types of

information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

11. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to Uintah, and thus Uintah was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

12. Upon information and belief, Uintah and its employees failed to properly implement security practices with regard to the computer network and systems that housed the Private Information. Had Uintah properly monitored its network, it could have prevented the Breach, or could have at least discovered it sooner.

13. Plaintiffs' and Class Members' identities are now at risk because of Uintah's negligent conduct as the Private Information that Uintah collected and maintained is now in the hands of data thieves and other unauthorized third parties.

14. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

PARTIES

15. Plaintiffs are, and at all times mentioned herein were, individual citizens of the State of Utah.

16. Defendant Uintah is a Utah corporation and a healthcare system with its principal place of business at 250 West 300 North, Roosevelt, UT 84066 in Duchesne County.

JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of

interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Uintah. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

18. This Court has jurisdiction over Uintah because Uintah operates in and/or is incorporated in this District.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Uintah has harmed Class Members residing in this District.

FACTUAL ALLEGATIONS

A. Uintah's Business and Collection of Plaintiffs' and Class Members' Private Information

20. Uintah is a healthcare system that provides healthcare-related services, including fitness, clinical, and hospital services, to its patients.¹

21. As a condition of providing healthcare services, Uintah requires that its patients entrust it with highly sensitive personal and health information. In the ordinary course of receiving service from Uintah, Plaintiffs and Class Members were required to provide their Private Information to Defendant.

22. Because of the highly sensitive and personal nature of the information Uintah acquires and stores with respect to its patients, Uintah, upon information and belief, promises to, among other things: keep patients' Private Information private; comply with industry standards related to data security and the maintenance of its patients' Private Information; inform its patients of its legal duties relating to data security and comply with all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that

¹ See <https://ubh.org/> (last visited on May 18, 2023).

relate to the services it provides; and provide adequate notice to patients if their Private Information is disclosed without authorization.

23. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Uintah assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

24. Plaintiffs and Class Members relied on Uintah to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

B. The Data Breach and Defendant's Inadequate Notice to Plaintiffs and Class Members

25. According to Defendant's Notice, it learned of unauthorized access to its computer systems on November 7, 2022.

26. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including names, Social Security numbers, dates of birth, medical treatment information, and health insurance information.

27. In or around early May of 2023, roughly six (6) months after Uintah learned that the Class's Private Information was first accessed by cybercriminals, Uintah finally began to notify patients that its investigation determined that their Private Information was compromised.²

28. Uintah delivered Data Breach Notification Letters to Plaintiffs and Class Members, alerting them that their highly sensitive Private Information "may have been accessed or acquired

² See <https://ago.vermont.gov/sites/ago/files/2023-05/2023-05-09%20Uintah%20Basin%20Healthcare%20Data%20Breach%20Notice%20to%20Consumers.pdf> (last visited on May 18, 2023).

without authorization during the incident.”³

29. The notice letter then included sections entitled “What We Are Doing” and “What You Can Do,” which listed generic and time-consuming steps that victims of data security incidents can take, such as getting a copy of a credit report, placing security freezes on credit reports, or notifying law enforcement about suspicious financial account activity. Other than providing only one year of credit monitoring that Plaintiffs and Class Members would have to affirmatively sign up for, and a call center number that victims could contact with questions, Uintah offered no other substantive steps to help victims like Plaintiffs and Class Members to protect themselves. On information and belief, Uintah sent a similar generic letter to all other individuals affected by the Data Breach.

30. Uintah had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs’ and Class Members’ Private Information confidential and to protect it from unauthorized access and disclosure.

31. Plaintiffs and Class Members provided their Private Information to Uintah with the reasonable expectation and mutual understanding that Uintah would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

32. Uintah’s data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

33. Uintah knew or should have known that its electronic records would be targeted by cybercriminals.

³ *Id.*

C. *The Healthcare Sector is Particularly Susceptible to Data Breaches*

34. Uintah was on notice that companies in the healthcare industry are susceptible targets for data breaches.

35. Uintah was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that “[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI).”⁴

36. The American Medical Association (“AMA”) has also warned healthcare companies about the importance of protecting their patients’ confidential information:

Cybersecurity is not just a technical issue; it’s a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients’ health and financial information, but also patient access to care.⁵

37. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.⁶ In 2022, the largest

⁴ Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), available at <https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820> (last visited on May 15, 2023).

⁵ Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass’n. (Oct. 4, 2019), available at: <https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals> (last visited on May 15, 2023).

⁶ Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, available at: <https://www.idtheftcenter.org/2018-data-breaches/> (last visited on May 15, 2023).

growth in compromises occurred in the healthcare sector.⁷

38. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the “average total cost to resolve an identity theft-related incident ... came to about \$20,000,” and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.⁸

39. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.⁹

40. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. “Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.”¹⁰

⁷ Identity Theft Resource Center, *2022 End-of-Year Data Breach Report*, available at: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on May 15, 2023).

⁸ Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), available at: <https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/> (last visited on May 15, 2023).

⁹ *Id.*

¹⁰ Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, available at: <https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks> (last visited on May 15, 2023).

41. As a healthcare provider, Uintah knew, or should have known, the importance of safeguarding its patients' Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on Uintah's patients as a result of a breach. Uintah failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

D. Uintah Failed to Comply with HIPAA

42. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq.* These provisions require that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI similar to the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

43. Uintah's Data Breach resulted from a combination of insufficiencies that indicate Uintah failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Uintah's Data Breach that Uintah either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiffs' and Class Members' PHI.

44. Plaintiffs' and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

45. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

46. 45 CFR § 164.402 defines “unsecured protected health information” as “protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]”

47. Plaintiffs’ and Class Members’ Private Information included “unsecured protected health information” as defined by 45 CFR § 164.402.

48. Plaintiffs’ and Class Members’ unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

49. Based upon Defendant’s Notice to Plaintiffs and Class Members, Uintah reasonably believes that Plaintiffs’ and Class Members’ unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

50. Plaintiffs’ and Class Members’ unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

51. Uintah reasonably believes that Plaintiffs’ and Class Members’ unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

52. Plaintiffs’ and Class Members’ unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

53. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

54. Uintah reasonably believes that Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

55. It is reasonable to infer that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

56. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

57. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

58. In addition, Uintah's Data Breach could have been prevented if Uintah had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients.

59. Uintah's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

- b. Failing to mitigate the risks of a data breach and loss of data;
- c. Failing to ensure the confidentiality and integrity of electronic protected health information Uintah creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);
- d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);
- e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);
- f. Failing to identify and respond to suspected or known security incidents;
- g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);
- h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);
- i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);
- j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

- k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

60. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 also required Uintah to provide notice of the Data Breach to each affected individual “without unreasonable delay and *in no case later than 60 days following discovery of the breach*” (emphasis added).

61. Because Uintah has failed to comply with HIPAA, while monetary relief may cure some of Plaintiffs’ and Class Members’ injuries, injunctive relief is also necessary to ensure Uintah’s approach to information security is adequate and appropriate going forward. Uintah still maintains the PHI and other highly sensitive PII of its current and former patients, including Plaintiffs and Class Members. Without the supervision of the Court through injunctive relief, Plaintiffs’ and Class Members’ Private Information remains at risk of subsequent data breaches.

E. Uintah Failed to Comply with FTC Guidelines

62. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

63. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep,

properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

64. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

65. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

66. As evidenced by the Data Breach, Uintah failed to properly implement basic data security practices. Uintah's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

67. Uintah was at all times fully aware of its obligation to protect the Private Information of its patients yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Uintah Failed to Comply with Industry Standards

68. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

69. Some industry best practices that should be implemented by businesses dealing with sensitive PHI like Uintah include but are not limited to educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

70. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

71. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

72. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

G. Uintah Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information

73. In addition to its obligations under federal and state laws, Uintah owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Uintah owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

74. Uintah breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Uintah's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect patients' Private Information;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to sufficiently train its employees regarding the proper handling of its patients Private Information;
- e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

- f. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and
- g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

75. Uintah negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

76. Had Uintah remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

77. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with Uintah.

H. Uintah Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft

78. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.¹¹ Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the

¹¹ *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), available at https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on May 15, 2023).

ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and/or services available which can have negative impacts on daily life.

79. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

80. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

81. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

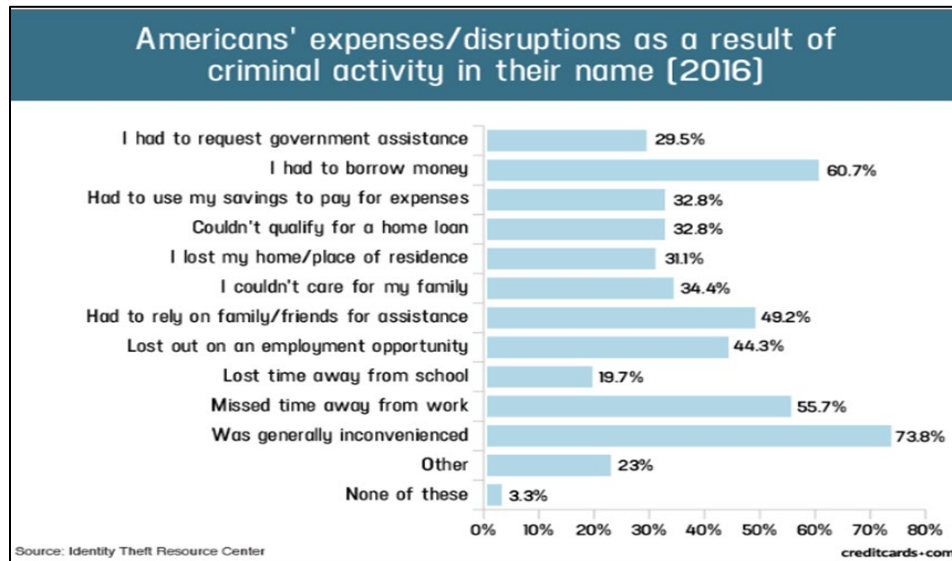
82. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

83. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.¹² However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

84. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

¹² See *IdentityTheft.gov*, Federal Trade Commission, available at <https://www.identitytheft.gov/Steps> (last visited May 15, 2023).

85. In fact, a study by the Identity Theft Resource Center¹³ shows the multitude of harms caused by fraudulent use of PII:



86. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.¹⁴

87. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

88. While credit card information and associated PII can sell for as little as \$1-\$2 on the black market, protected health information can sell for as much as \$363 according to the Infosec Institute.¹⁵

¹³ Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), available at <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/> (last visited on May 15, 2023).

¹⁴ Federal Trade Commission, *Warning Signs of Identity Theft*, available at: <https://consumer.ftc.gov/articles/what-know-about-identity-theft> (last visited on May 15, 2023).

¹⁵ Center for Internet Security, *Data Breaches: In the Healthcare Sector*, available at: <https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector> (last visited on May 15, 2023).

89. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

90. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."¹⁶

91. The ramifications of Uintah's failure to keep its current and former patients' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

92. Here, not only was sensitive medical information compromised, but Social Security numbers were compromised too. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

93. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is

¹⁶ Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: <https://kffhealthnews.org/news/rise-of-identity-theft/> (last visited on May 15, 2023).

misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:¹⁷

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

94. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

95. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

I. Plaintiffs' and Class Members' Damages

96. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

97. Plaintiffs and Class Members entrusted their Private Information to Defendant in order to receive healthcare services from Defendant.

98. Plaintiffs' Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

¹⁷ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), available at <https://www.gao.gov/assets/270/262904.html> (last visited May 15, 2023).

99. As a direct and proximate result of Uintah's actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

100. Further, as a direct and proximate result of Uintah's conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach.

101. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

102. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

103. Plaintiffs and Class Members also lost the benefit of the bargain they made with Uintah. Plaintiffs and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price paid to Uintah by or on behalf of Plaintiffs and Class Members was intended to be used by Uintah to fund adequate security of Uintah's system and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class did not receive the benefit of the bargain.

104. Additionally, Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and records including, *e.g.*, medical records and explanations of benefits, for misuse.

105. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

- a. Monitoring for and discovering fraudulent charges;
- b. Canceling and reissuing credit and debit cards;
- c. Purchasing credit monitoring and identity theft prevention;
- d. Addressing their inability to withdraw funds linked to compromised accounts;
- e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
- f. Placing “freezes” and “alerts” with credit reporting agencies;
- g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;
- h. Contacting financial institutions and closing or modifying financial accounts;
- i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

- j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and
- k. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

106. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Uintah, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal and health information of its patients is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

107. As a direct and proximate result of Uintah's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

CLASS ACTION ALLEGATIONS

108. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Fed. R. Civ. P. 23(a), (b)(1), (b)(2), and (b)(3).

109. Specifically, Plaintiffs propose the following Nationwide Class, (also referred to herein as the "Class"), subject to amendment as appropriate:

Nationwide Class

All individuals residing in the United States who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

110. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

111. Plaintiffs reserve the right to modify or amend the definitions of the proposed Nationwide Class and add subclasses, if necessary, before the Court determines whether certification is appropriate.

112. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23.

113. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of over 103,000 current and former patients of Uintah whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Uintah's records, Class Members' records, publication notice, self-identification, and other means.

114. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Uintah engaged in the conduct alleged herein;
- b. Whether Uintah's conduct violated the FTCA or HIPAA;
- c. When Uintah learned of the Data Breach
- d. Whether Uintah's response to the Data Breach was adequate;
- e. Whether Uintah unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

- f. Whether Uintah failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;
- g. Whether Uintah's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- h. Whether Uintah's data security systems prior to and during the Data Breach were consistent with industry standards;
- i. Whether Uintah owed a duty to Class Members to safeguard their Private Information;
- j. Whether Uintah breached its duty to Class Members to safeguard their Private Information;
- k. Whether hackers obtained Class Members' Private Information via the Data Breach;
- l. Whether Uintah had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;
- m. Whether Uintah breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;
- n. Whether Uintah knew or should have known that its data security systems and monitoring processes were deficient;
- o. What damages Plaintiffs and Class Members suffered as a result of Uintah's misconduct;
- p. Whether Uintah's conduct was negligent;
- q. Whether Uintah's conduct was *per se* negligent;

- r. Whether Uintah was unjustly enriched;
- s. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;
- t. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and
- u. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

115. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Uintah. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

116. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

117. Predominance. Uintah has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Uintah's conduct affecting Class Members set out above predominate over any

individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

118. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Uintah. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

119. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Uintah has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

120. Finally, all members of the proposed Class are readily ascertainable. Uintah has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Uintah.

FIRST CAUSE OF ACTION **Negligence (On behalf of Plaintiffs and the Class)**

121. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

122. Uintah knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

123. Uintah's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

124. Uintah knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Uintah was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

125. Uintah owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. Uintah's duties included, but were not limited to, the following:

- a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;
- b. To protect patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;
- c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;
- d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the FTCA;
- e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

- f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

126. Uintah's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

127. Uintah's duty also arose because Defendant was bound by industry standards to protect its patients' confidential Private Information.

128. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Uintah owed them a duty of care to not subject them to an unreasonable risk of harm.

129. Uintah, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Uintah's possession.

130. Uintah, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

131. Uintah, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

132. Uintah breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to comply with the FTCA;
- f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and
- g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

133. Uintah acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiffs and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

134. Uintah had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Uintah with their Private Information was predicated on the understanding that Uintah would take adequate security precautions. Moreover, only Uintah had the ability to protect its systems (and the Private Information that it stored on them) from attack.

135. Uintah's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised, exfiltrated, and/or misused, as alleged herein.

136. As a result of Uintah's ongoing failure to notify Plaintiffs and Class Members regarding exactly what Private Information has been compromised, Plaintiffs and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

137. Uintah's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

138. As a result of Uintah's negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

139. Uintah also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

140. As a direct and proximate result of Uintah's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

141. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

142. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

143. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Uintah to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

SECOND CAUSE OF ACTION

Negligence *Per Se* (On behalf of Plaintiffs and the class)

144. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

145. Pursuant to Section 5 of the FTCA, Uintah had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

146. Pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq.*, Uintah had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

147. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

148. Uintah breached its duties to Plaintiffs and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

149. Specifically, Uintah breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to: proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

150. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The

FTC rulings and publications described above and the industry-standard cybersecurity measures also set forth above form part of the basis of Uintah's duty in this regard.

151. Uintah also violated the FTCA and HIPAA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

152. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Uintah's networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

153. Plaintiffs and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect and Uintah's failure to comply with both constitutes negligence *per se*.

154. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to Uintah's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

155. As a direct and proximate result of Uintah's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

156. As a direct and proximate result of Uintah's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

157. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Uintah to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

THIRD CAUSE OF ACTION

Breach of Implied Contract (On behalf of Plaintiffs and the class)

158. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

159. Uintah provides healthcare services to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiffs and Class Members paying for healthcare services from Defendant.

160. Through Defendant's provision of healthcare services to its patients, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Private Information in accordance with its policies, practices, and applicable law.

161. As consideration, Plaintiffs and Class Members paid money to Uintah and turned over valuable Private Information to Uintah. Accordingly, Plaintiffs and Class Members bargained with Uintah to securely maintain and store their Private Information.

162. Uintah accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing healthcare services to Plaintiffs and Class Members.

163. In delivering their Private Information to Uintah and paying for healthcare services, Plaintiffs and Class Members intended and understood that Uintah would adequately safeguard the Private Information as part of that service.

164. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; (7) complying with HIPAA standards to make sure that Plaintiffs' and Class Members' PHI would remain protected; and (8) taking other steps to protect against foreseeable data breaches.

165. Plaintiffs and Class Members would not have entrusted their Private Information to Uintah in the absence of such an implied contract.

166. Had Uintah disclosed to Plaintiffs and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their Private Information to Uintah.

167. As a provider of healthcare services, Uintah recognized (or should have recognized) that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and the other Class Members.

168. Uintah violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information. Uintah further breached these implied contracts by failing to comply with its promise to abide by HIPAA.

169. Additionally, Uintah breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

170. Uintah also breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

171. Uintah further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

172. Uintah further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

173. Uintah further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

174. Uintah further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

175. Uintah further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations, in violation of 45 CFR 164.306(a)(94).

176. Uintah further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

177. Uintah further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR 164.530(c).

178. Uintah further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PHI.

179. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide accurate and complete Private Information and to pay Uintah in exchange for Uintah's agreement to, *inter alia*, protect their Private Information.

180. Plaintiffs and Class Members have been damaged by Uintah's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

FOURTH CAUSE OF ACTION
Unjust Enrichment (On behalf of Plaintiffs and the class)

181. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

182. This Count is pleaded in the alternative to the Third Cause of Action above.

183. Plaintiffs and Class Members conferred a benefit on Uintah by turning over their Private Information to Defendant and by paying for healthcare services that should have included

cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

184. Upon information and belief, Uintah funds its data security measures entirely from its general revenue, including from payments made to it by or on behalf of Plaintiffs and Class Members.

185. As such, a portion of the payments made by or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Uintah.

186. Uintah has retained the benefits of its unlawful conduct, including the amounts of payment received from or on behalf of Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

187. Uintah knew that Plaintiffs and Class Members conferred a benefit upon it, which Uintah accepted. Uintah profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

188. If Plaintiffs and Class Members had known that Uintah had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant and would have gone elsewhere to receive healthcare services.

189. Due to Uintah's conduct alleged herein, it would be unjust and inequitable under the circumstances for Uintah to be permitted to retain the benefit of its wrongful conduct.

190. As a direct and proximate result of Uintah's conduct, Plaintiffs and Class Members have suffered and/or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Uintah's possession and is subject to further unauthorized disclosures so long as Uintah fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

191. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Uintah and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Uintah from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

192. Plaintiffs and Class Members may not have an adequate remedy at law against Uintah, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

FIFTH CAUSE OF ACTION

Breach of Confidence (On behalf of Plaintiffs and the Class)

193. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

194. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by Uintah and ultimately accessed and acquired in the Data Breach.

195. As a healthcare provider, Uintah has a special, fiduciary relationship with its patients, including Plaintiffs and Class Members. Because of that special relationship, Uintah was provided with and stored Plaintiffs' and Class Members' Private Information and had a duty to maintain such Information in confidence.

196. Patients like Plaintiffs and Class Members have a privacy interest in personal medical and other matters, and Uintah had a duty not to disclose such matters concerning its patients.

197. As a result of the parties' relationship, Uintah had possession and knowledge of highly sensitive and confidential PHI and PII belonging to Plaintiffs and Class Members, information that was not generally known.

198. Plaintiffs and Class Members did not consent nor authorize Defendant to release or disclose their Private Information to an unknown criminal actor.

199. Uintah breached its duty of confidence owed to Plaintiffs and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of Plaintiffs' and Class Members' Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards

in place to control these risks; (c) failing to design and implement adequate information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) making an unauthorized and unjustified disclosure and release of Plaintiffs' and Class members' Private Information to a criminal third party.

200. But for Uintah's wrongful breach of its duty of confidence owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

201. As a direct and proximate result of Uintah's wrongful breach of its duty of confidence, Plaintiffs and Class Members have suffered and will continue to suffer the injuries alleged herein.

202. It would be inequitable for Uintah to retain the benefit of controlling and maintaining Plaintiffs' and Class Members' Private Information at the expense of Plaintiffs and Class Members.

203. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

- a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and

finding that Plaintiffs are proper representatives of the Nationwide Class requested herein;

- b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;
- c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;
- d. An order instructing Uintah to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;
- e. An order requiring Uintah to pay the costs involved in notifying Class Members about the judgment and administering the claims process;
- f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and
- g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED this 19th day of May, 2023.

MARSHALL OLSON & HULL, PC

BY: /s/ Jason R. Hull
JASON R. HULL

SIRI & GLIMSTAD LLP

MASON A. BARNEY
TYLER J. BEAN

ATTORNEYS FOR PLAINTIFFS AND PROPOSED CLASS
COUNSEL